REMARKS

[0002] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Applicant submits the remarks and amendments made herein should be entered as they are accompanied by a Request for Continued Examination and the appropriate fee. The status of the claims is as follows:

- Claims 1-13, 19-29 and 31-40 are currently pending.
- No claims are canceled herein.
- No claims are withdrawn herein.
- Claim 1 is amended herein.
- No new claims are added herein.

Cited Document

[0003] The Examiner's rejections are based upon the following reference:

- **Sankar**: Sankar, U.S. Patent No. 7,065,706.

[0004] Applicant notes that Sankar is directed to a network router for use in an open protocol network. The disclosed router is described as being configured for executing network operations (e.g. routing requests and responses) for network nodes utilizing XML (Sankar, Field of the Invention).

[0005] Sankar discloses that such a router must be capable of parsing XML messages (Col. 2, ll. 24-28). In describing the particular need for the router's XML parsing features, Sankar describes the need to identify the relevant attributes of a message such as a "security attribute" in order to perform certain operations.

[0006] As such, Sankar is, at best, only loosely related to the instant application, which "relates generally to security systems for computing environments" (Application, p. 1 "Field").

[0007] Applicant notes the forgoing to provide the proper context for understanding the disclosure of Sankar.

Claims Rejected Based on Sankar

[0008] Claims 1-13, 19-29 and 31-40 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Sankar. Applicant respectfully traverses the rejection.

[0009] Here Applicant reiterates from the response filed 06/30/09 that the rejections of the claims do not address all of the claimed features and elements of the claims. For this reason alone, the Examiner has failed to establish prima facie anticipation from Sankar. However, Applicant additionally submits the following remarks.

Independent Claim 1

[0010] Applicant submits that the Office has not shown that Sankar anticipates this claim, as Sankar does not disclose at least the following features of this claim (with emphasis added):

- "on a device ***configured as part of a security infrastructure*** to receive messages, receiving a message;"
- "***selecting a first set of security information*** from a first plurality of sets of security information as a function of a property of the message, wherein the first set of security information comprises security settings;
- **selecting a second set of security information** from a second plurality of sets of security information as a function of the first set, wherein the second set of security information comprises security settings ***and wherein the second set is a distinct set from that of the first set***;"

[0011] The Examiner indicates (Action, p. 4) the following with regard to this claim:

Regarding claim 1, Sankar discloses:

A method, comprising:

on a device configured to receive messages, receiving a message (column 2, lines 35-39: *received message*);

selecting a first set of security information (column 2, lines 25-35: *parsing XML tags to get information*) from a first plurality of sets of security information (column 2, lines 25-35: *XML tags*) as a function of a property of the message (column 2, lines 25-40: *wherein the message is received and then the XML tags are parsed*);

selecting a second set of security information (column 2, lines 35-40: *retrieving the attributes (second set of security information) from the XML tags and determining identifying relevant attributes (selecting second set))* from a second plurality of sets of security information (column 2, lines 35-40: *retrieving all the attributes*) as a function of the first set (column 2, lines 24-48: *wherein the attributes are retrieved by parsing the XML tags*); and

applying the second set of security information to the message (column 2, lines 43-46: *determining security attributes to determine the operation to be performed on the message*).

[0012] Firstly, Applicant notes the Examiner has not addressed the specific language of the claim. For example, the claim expressly recites "on a device configured as part of a security infrastructure to receive messages, receiving a message." It is apparent from a cursory review of the rejection, that this claim language has not been addressed by the rejection. For this reason alone, prior to amendment herein, the claim has not been shown to have been anticipated and is therefore patentable over the cited reference.

[0013] Additionally, in the "Response to Arguments, p. 2-3, the Examiner concedes the following:

> "The Examiner interprets security settings as information that is parsed to determine what security is to be applied. Given this interpretation, the XML tags, which ***contain security attributes***, are interpreted as the first security information" (emphasis added).

[0014] As can be seen from the rejection, the Examiner equates the "XML tags" disclosed by Sankar with the claimed "first set of security information" and the "attributes" disclosed by Sankar as being equivalent to the claimed "second set of security information". Applicant respectfully disagrees.

[0015] Sankar expressly states "[t]he router includes an XML parser configured for parsing XML tags specifying prescribed attributes..." (Col. 2, ll. 28-29). While it is true that Sankar discloses that one of the "attributes" of a message can be "security attributes" (Col. 2, line 46), according to Sankar the XML tags are merely a container for attributes generally and security attributes in some cases. Applicant notes the Examiner concedes that the disclosed XML tags are merely a container.

[0016] The "XML tags" and the "attributes" are therefore not a first and second set of security information. The only "set" of security information that one of ordinary skill in the art would understand from Sankar's disclosure, would arguably be the "security attribute".

[0017] Furthermore, the claim, as amended herein, expressly requires that "the second set is a distinct set from that of the first set".

[0018] Since Sankar at best only discloses one set of security information; namely "security attributes", and that it is contained by the XML tags, it can not be fairly said that Sankar anticipates this claim, because, the XML tags do not contain security information that is distinct from the security attributes.

[0019] Furthermore, the claim expressly recites that the selection is "from a first *plurality* of sets of security information". At best, Sankar only discloses a *singular* set of security information (namely the "security attributes"), therefore it would be impossible to select from a *plurality* of sets.

[0020] Applicant additionally notes that the claim recites "wherein the first set of security information comprises security settings". Here yet a third distinction exists because not only are the XML tags of Sankar not security information, they are not described as being security information comprised of security settings. At best they only *contain* security information that defines security settings. The "XML tags" of Sankar are not security information in and of themselves, and are not additionally comprised of security settings as claimed.

[0021] As such, Sankar is wholly inadequate to anticipate the portions of the claim actually addressed by the rejection (even prior to amendment). Consequently, this claim is patentable over the cited reference. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim and pass the case along to issuance.

Dependent Claims 2-13

[0022] These claims ultimately depend upon independent claim 1. As discussed above, claim 1 is patentable. It is axiomatic that any dependent claim, which depends from an patentable base claim, is also patentable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Independent Claim 19

[0023] Applicant submits that the Office has not shown that Sankar anticipates independent claim 19, as Sankar does not disclose at least the following features of this claim (with emphasis added):

- a first datastore to include ***a first plurality of sets of security settings*** related to an application residing in the system, wherein the first plurality of sets define messages that must be secured;
- a second datastore to include ***a second plurality of sets of security settings***, wherein the second plurality of sets specify settings and operations for securing messages, and wherein a set of the first plurality of sets is associated with a set of the second plurality of sets;

[0024] The Examiner indicates (Action, pp. 8-9) the following with regard to this claim:

Regarding claim 19, Sankar discloses:

A system comprising:

a processor (column 4, lines 8-15);

a memory coupled to the processor to store at least a portion of a plurality of datastores (column 4, lines 8-15);

a first datastore to include a first plurality of sets of security information (column 2, lines 25-35: *parsing XML tags to get information*) related to an application residing in the system (column 2, lines 25-40: *wherein the message is received and then the XML tags are parsed to determine which application/process the message is to be re-routed to*);

a second datastore to include a second plurality of sets of security information (column 2, lines 35-40: *retrieving the attributes (second set of security information)*, wherein a set of the first plurality of sets is associated with a set of the second plurality of sets (column 2, lines 24-48: *wherein the attributes are retrieved by parsing the XML tags*); and

a module to select a first set from the first plurality of sets as a function of a property of a received message (column 2, lines 25-40: *wherein the message is received and then the XML tags are parsed*).

[0025] Here, as can be seen, the Examiner again asserts that because the XML tags are described as being parsed to determine routing information and security attributes, that this constitutes the claimed first and second plurality of sets of security "information". Applicant again respectfully disagrees. Applicant submits, that at best, the XML tags would more closely correspond to either the first or second (not both) datastores that include security settings. Applicant submits this without concession.

[0026] Applicant notes that XML and XML tags are well known in the art, and one of ordinary skill in the art would not interpret XML tags in and of themselves to be security information. For example, the Computer Desktop Encyclopedia states the following with regard to XML documents and XML tags:

> A file that contains text with interspersed descriptions, called "tags." All XML files are XML documents and vice versa. The XML document is often organized in a hierarchy with an "open" tag at the beginning of the file, a "close" tag at the end and all the text elements in between. Each text element has an open and close tag as well, and all tags begin with the less-than (<) character and end with the greater-than (>) character.
>
> XML Tag Example
>
> This example shows one definition from the XML feed for this encyclopedia. All the tags within the open and close "definition" tags are in a prescribed hierarchy. Note that all close tags have a slash (/) after the beginning less-than (<) symbol.[1]

[0027] As can be seen, XML tags are known to be merely a part of an organizational hierarchy that define descriptions. Broadly, and in keeping with the scope of Sankar's disclosure, XML tags may contain descriptions that are "security attributes"

[0028] In spite of this, the Examiner has interpreted the XML tags of Sankar themselves as security settings because XML tags are described therein as being parsed to determine what security is to be applied (by virtue of the security attributes contained therein). Given the above definition, and even the Examiner's interpretation, the XML tags can not be the claimed "first plurality of sets of security settings" if the second set is the "security attribute" contained therein. More appropriately, one of ordinary skill in the art would interpret the XML tags as being merely a container for security settings (as conceded by the Examiner, Action p. 3). By definition, a container is not the thing that it contains. Therefore, the XML tags themselves are not security settings.

[0029] Not having shown the claimed "first plurality of sets of security setting"s, Applicant reiterates that the reference does not describe “a second plurality of sets of security settings”.

[0030] For the forgoing reasons, Sankar does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

---

[1] "XML document." Computer Desktop Encyclopedia. Computer Language Company Inc., 2009. *Answers.com* 27 Oct. 2009. http://www.answers.com/topic/xml-document

Dependent Claims 20-29

[0031] These claims ultimately depend upon independent claim 19. As discussed above, claim 19 is allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Independent Claim 31

[0032] Applicant submits that the Office has not shown that Sankar anticipates this claim, as Sankar does not disclose the following features of this claim (with emphasis added):

- steps for selecting ***a first set of security information from a first plurality of sets of security information*** as a function of a property of the message, ***wherein the first set of security information comprises security settings that define types of messages that must be secured*** and wherein the types of messages that must be secured are defined and provided by an application developer;
- steps for ***selecting a second set of security information from a second plurality of sets of security information*** as a function of the first set, wherein the second set of security information comprises security settings that specify particular operations and settings for securing the messages, wherein the particular operations and settings comprise algorithms to be used in signing and encrypting the messages; and
- ***steps for applying the second set of security information*** to the message.

[0033] The Examiner indicates (Action, pp. 12-13) the following with regard to this claim:

> Regarding claim 31, Sankar discloses:
>
> A machine-readable medium having components, comprising:
>
> steps for receiving a message (column 2. lines 35-39: *received message*);

steps for selecting a first set of security information (column 2, lines 25-35: *parsing XML tags to get information*) from a first plurality of sets of security information (column 2, lines 25-35: *XML tags*) as a function of a property of the message (column 2, lines 25-40: *wherein the message is received and then the XML tags are parsed*), wherein the first set of security information comprises security settings that define types of messages that must be secured and wherein the types of messages that must be secured are defined and provided by an application developer (column 2, lines 25-35: *parsing XML tags to get information about what security functions to perform on the message*);

steps for selecting a second set of security information (column 2, lines 35-40: *retrieving the attributes (second set of security information) from the XML tags and determining identifying relevant attributes (selecting second set))* from a second plurality of sets of security information (column 2, lines 35-40: *retrieving all the attributes*) as a function of the first set (column 2, lines 24-48: *wherein the attributes are retrieved by parsing the XML tags*), wherein the second set of security settings that specify particular operations and settings for securing the messages, wherein the particular operations and settings comprise algorithms to be used in signing and encrypting the messages (column 4, lines 7-26: *XML encryption and XML signature are functions provided for by the message router and stored on a registry server*); and

means for applying the second set of security information to the message (column 2, lines 43-46: *determining security attributes to determine the operation to be performed on the message).*

[0034] Firstly, Applicant here notes the Examiner appears to be rejecting claim language not found in the currently pending claim. Applicant specifically refers to where the Examiner rejects "means for applying" when the claim expressly recites "steps for applying". Applicant notes that this oversight has persisted through the last 2 (two) office actions. Not having addressed the claimed "steps for applying", Applicant submits this claim is patentable over the cited reference.

[0035] Secondly, Applicant reiterates that Sankar simply does not disclose a plurality of sets of security information, as established above.

[0036] Furthermore, to reject the claimed:

- "wherein the first set of security information comprises security settings that define types of messages that must be secured and wherein the types of messages that must be secured are defined and provided by an application developer",

[0037] the Examiner cites to Sankar col. 2 ll. 25-35. This portion of Sankar is reproduced below:

> There also is a need for an arrangement that enables a router in an open protocol network to request services, based on execution of prescribed applications by remote nodes on the open protocol network, based on parsing a received XML document. These and other needs are attained by the present invention, where a router is configured for routing, via an open protocol network, a received message to a destination node based on parsing an XML portion within the received message. The router includes an XML parser configured for parsing XML tags specifying prescribed attributes, and an application resource configured for interpreting the prescribed attributes for a determined service based on runtime execution of the application resource. In particular, the runtime execution of the application resource provides application-specific syntax and semantics enabling interpretation of the parsed XML tags. The application resource, in response to interpreting the prescribed attributes, initiates selected application operations, including outputting the received message to a prescribed destination, based on the execution of the prescribed application operations."

[0038] As can be seen, there is no portion of this cited section which one of ordinary skill in the art would interpret as being the equivalent of the claimed "security settings that define ***types of messages*** that must be secured and wherein the types of messages that must be secured are defined and provided by an application developer". There disclosure does not even suggest that there are different types of messages, let alone that security settings define them as claimed.

[0039] Consequently, Sankar does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 32-40

[0040] These claims ultimately depend upon independent claim 31. As discussed above, claim 31 is allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Conclusion

[0041] In light of the forgoing amendments and remarks, early reconsideration and allowance of this application are most courteously solicited. Should the Examiner feel that a personal discussion might be helpful in advancing this case to allowance, they are invited to telephone or e-mail the undersigned.

[0042] In addition, it is believed that all of the pending claims have been fully addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed.

[0043] Finally, nothing in this communication should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this communication, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/Randall T. Palmer 61440/ Dated: 10/29/09

Randall T. Palmer
(randy@leehayes.com; 509-944-4761)
Registration No. 61440

Rob Peck
(robp@leehayes.com; 206-876-6019)
Registration No. 56826